withdrawn from the account involved without the account owner being notified and/or having a say in the matter.

[0012] The account owners are typically notified of the above-described activity involving their account days later when they either receive a mailed notice and/or when they receive and review their monthly or periodic statement, which notice may be received at a time when it may be too late for the account owner to stop or reverse the transaction and/or, in the case of a check or draft returned for insufficient funds, at a time which is too late for the account owner to attempt to collect the funds. In the case of automated teller machine accounts, these accounts may be accessed, such as with a lost, stolen, or counterfeit card and/or with a card account number(s) and/or associated personal identification number(s), by a thief or by any other unauthorized person who could then make an unauthorized withdrawal(s) therefrom.

[0013] Once again, account owners would not receive notification and/or have knowledge of the unauthorized transaction until they are notified by the bank or financial institution either via a monthly and/or periodic statement, and/or when they attempt a transaction at the automated teller machine and, at that time, discover that funds are missing and/or have been withdrawn. In the case of savings accounts, checking accounts and/or automated teller machine accounts, there is no present apparatus or method by which to link the location of a communication device with authorization of a transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

[0015] **FIG. 1** is a block diagram of a network suitable for use in the present invention;

[0016] **FIG. 2** is a block diagram of components found in **FIG. 1**;

[0017] **FIG. 3** is a flow chart illustrating the steps taken in one embodiment of the present invention; and

[0018] **FIG. 4** is a block diagram of an exemplary database **106** found in **FIG. 1**.

SUMMARY OF THE INVENTION

[0019] One aspect of the present invention relates to a method for authorizing transactions against an account. The account may be a credit, debit or other transaction account. A transaction is received that includes a request for authorization to charge an amount against the account. An ID for a communication device associated with the account is retrieved and the location of the communication device is determined. The location of the transaction is determined and compared with the location of the device. The request is then processed based on the location information received. The request is preferably denied when the location of the transaction is different from the location of the device. Alternatively, the request preferably is authorized when the location of the transaction is the same as the location of the device.

[0020] A system for authorizing transactions against an account is also provided. The system includes an input device adapted to receive a transaction that includes a request for authorization to charge an amount against the account. A means for retrieving an ID for a communication device associated with the account is provided. The input device is coupled for data communications with the retrieving means. A means for determining the location of the communication device, a means for determining the location of the transaction, a means for comparing the location of the transaction with the location of the device, and a means for processing the request are also provided.

[0021] All objects, features, and advantages of the present invention will become apparent in the following detailed written description.

DETAILED DESCRIPTION OF THE INVENTION

[0022] The present invention is directed to a system and method for reducing fraudulent transactions involving credit or debit type transaction cards. Briefly, the location of the transaction is compared to the real time physical location of a pre-defined communication device. Where the locations are the same, the transaction is authorized and where the locations are not the same, the transaction is denied. A transaction card account holder may set one or more device locations for verifying the location of the card holder at the time of a transaction.

[0023] With reference now to the figures, and, in particular, with reference now to **FIG. 1**, there is depicted a block diagram of a network environment in which the present invention may be implemented. While the present invention is described with reference to one type of network environment, it will be understood by one with skill in the art that the present invention may be implemented in alternate types of network environments.

[0024] **FIG. 1** is a schematic diagram of a network in accordance with one embodiment of the present invention. The figures describe the present invention with reference to a merchant transaction however, it should be noted that the invention is applicable to transactions where a merchant is not present, for example, a transaction at an automated teller machine. A transaction card is initially read at a point of sale terminal **102** at a merchant's location. The point of sale terminal **102**, contacts a transaction service provider or central computer **104**, typically via a telephone call. When the phone call is connected, the point of sale terminal **102** initializes communication with the service provider central computer **104**. The service provider typically validates the transaction card. This may include checking with the actual card issuer to make sure the proposed procurement would not exceed predetermined maximum purchase limits. The central computer **104** may contain a database **106** containing at least one device ID **114** for an account holder's communication device **112** and optionally a database **108** containing card limits.

[0025] The point-of-sale authorization terminal **102** may be any of the widely used and well known terminals or